The Rational Numbers as an Abstract Data Type

J. A. BERGSTRA

University of Amsterdam, Informatics Institute, Amsterdam, The Netherlands

AND

J. V. TUCKER

University of Wales Swansea, Singleton Park, Swansea, United Kingdom

Abstract. We give an equational specification of the field operations on the rational numbers under initial algebra semantics using just total field operations and 12 equations. A consequence of this specification is that $0^{-1} = 0$, an interesting equation consistent with the ring axioms and many properties of division. The existence of an equational specification of the rationals *without hidden functions* was an open question. We also give an axiomatic examination of the divisibility operator, from which some interesting new axioms emerge along with equational specifications of algebras of rationals, including one with the modulus function. Finally, we state some open problems, including: Does there exist an equational specification of the field operations on the rationals without hidden functions that is a complete term rewriting system?

Categories and Subject Descriptors: D.3.1 [**Programming Languages**]: Formal Definition and Theory; D.3.3 [**Programming Languages**]: Language Constructs and Features; F.1.3 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs; F.3.2 [**Logics and Meanings of Programs**]: Semantics of Programming Languages; F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic

General Terms: Verification, Languages

Additional Key Words and Phrases: Rational numbers, field, meadow, division-by-zero, total versus partial functions, abstract data types, algebraic specification, equations, initial algebra, computable algebras

ACM Reference Format:

Bergstra, J. A. and Tucker, J. V. 2007. The rational numbers as an abstract data type J. ACM 54, 2, Article 7 (April 2007), 25 pages. DOI = 10.1145/1219092.1219095 http://doi.acm.org/10.1145/1219092.1219095

Authors' addresses: J. A. Bergstra, University of Amsterdam, Informatics Institute, Kruislaan 403, 1098 SJ Amsterdam, The Netherlands, e-mail: janb@science.uva.nl; J. V. Tucker, Department of Computer Science, University of Wales Swansea, Singleton Park, Swansea, SA2 8PP, United Kingdom, e-mail: j.v.tucker@swansea.ac.uk.

1. *Introduction*

Measurements are made using some kind of gauge. To calibrate a gauge, one chooses a unit and divides that unit into a number k of subunits of equal size. Then a measurement is denoted by n whole units and m subunits or, in this case, $n\frac{m}{k} = (nk + m)/k$ subunits. Note that measurements are finite.

The set $\mathbb{Q}$ of rational numbers is a number system designed to denote measurements. Most users make computations involving measurements. Hence, the set $\mathbb{Q}$ of rational numbers is among the truly fundamental data types. The rationals are the numbers with which we make finite computations in practice. Despite the fact they have been known and used for over two millennia, they are somewhat neglected in the modern theory of data types.

On the rationals, we calculate using standard operations such as the functions $+, -, \cdot, ^{-1}$. Algebras made by equipping $\mathbb{Q}$ with some selection of operations we call here *rational arithmetics*. The algebra $(\mathbb{Q} \mid 0, 1, +, -, \cdot, ^{-1})$ is usually called the *field* of rational numbers when the operations satisfy certain axioms.

In this article, we will model some rational arithmetics, including the field, as abstract data types. Now, the rationals can be specified by the field axioms; indeed, they are uniquely definable up to isomorphism as the prime subfield of characteristic 0. However, the field axioms contain a negative conditional formula for inverse, which is difficult to apply and automate in formal reasoning. Specifically, we are interested in finding equational specifications of rational arithmetics under initial algebra semantics. Such equational axiomatisations allow simple term rewriting systems for reasoning and computation. Surprisingly, after over 30 years of data type theory, questions such as "Does there exist such an equational specification without hidden functions of the field of rational numbers?" seem to be open.

According to our general theory of algebraic specifications for computable data types (e.g., Bergstra and Tucker [1982; 1983; 1987; 1995]), since the common rational arithmetics are computable algebras, they have various equational specifications under both initial and final algebra semantics. Computable rational arithmetics even have equational specifications that are also complete term rewriting systems (by Bergstra and Tucker [1995]). However, these general specification theorems for computable data types involve hidden functions and are based on equationally definable enumerations of data. Recently, in Moss [2001], algebraic specifications of the rationals were considered. Among several interesting observations, Moss showed that there exists an equational specification with just *one* unary hidden function. He used a special enumeration technique that reminds one of the general methods of Bergstra and Tucker [1995], but is based on a remarkable enumeration theorem for the rationals in Calkin and Wilf [2000]. He also gave specifications of rational arithmetics with a modulus operator and with a floor.

Here we prove:

THEOREM 1.1. *There exists a finite equational specification under initial algebra semantics, without hidden functions, of the rational numbers with field operations that are all total.*

Our axioms include the commutative ring axioms and some general rules for inverses from which it can be deduced that

$$0^{-1} = 0.$$

This equation is also true of the hidden function specification in Moss [2001]. The equation $0^{-1} = 0$ occurs in several other places as well, for reasons of technical convenience (e.g., Hodges [1993] and Harrison [1998]). Our proposed specification includes a special axiom that codes a representation of an infinite subset of positive rational numbers.

The pursuit of this result leads to a thorough axiomatic examination of the divisibility operator, in which some interesting new axioms and models are discovered. In particular, we introduce a class of commutative rings with interesting division properties, which we call *meadows*.

The structure of the article is this: In Section 2, we give the basic equations that define the rational arithmetic operations and define some of their properties. In Section 3, we give two equational specifications of the rational field without hidden functions, one recursive and infinite, and one finite. In Section 5, we give results on fields and equational subtheories of fields, and on other rational arithmetics. Finally, in Section 6, we discuss some open problems.

This article is the first of a series on equational specifications of the rational arithmetics and their extensions, see Bergstra and Tucker [2006a; 2006b] and Bergstra [2006], launched in 2005 by Bergstra and Tucker [2005]. It can be read as a sequel to Bergstra and Tucker [1987; 1995], which contains a literature survey and the complementary general results. We use only the basic ideas of initial algebra specification. However, with several unfamiliar axioms about the familiar inverse operator in action, care is needed in verifying equations and other formulae.

We thank Kees Middelburg, Yoram Hirschfeld and an anonymous referee for valuable comments on the subject.

2. *Axioms for Rational Arithmetic*

2.1. PRELIMINARIES ON ALGEBRAIC SPECIFICATIONS. We assume the reader is familiar with using equations and conditional equations and initial algebra semantics to specify data types. Some accounts of this are: Goguen et al. [1978], Meseguer and Goguen [1985], and Wirsing [1990].

The theory of algebraic specifications is based on theories of universal algebras (e.g., Wechler [1992] and Meinke and Tucker [1992]); computable and semicomputable algebras [Stoltenberg-Hansen and Tucker 1995]; and term rewriting [Klop 1992; Terese 2003].

We use standard notations: typically, we let Σ be a many sorted signature and A a total Σ algebra. The class of all total Σ algebras is $Alg(\Sigma)$ and the class of all total Σ algebras satisfying all the axioms in a theory T is $Alg(\Sigma, T)$. The word "algebra" will mean total algebra.

2.2. ALGEBRAIC SPECIFICATIONS OF THE RATIONALS. We will build our specifications in stages. The primary signature Σ is simply that of the *field* of rational numbers:

signature Σ
sorts *field*
operations
$0: \rightarrow$ *field*;
$1: \rightarrow$ *field*;

$+$: *field* $\times$ *field* $\to$ *field*;
$-$: *field* $\to$ *field*;
$\cdot$: *field* $\times$ *field* $\to$ *field*;
$^{-1}$: *field* $\to$ *field*
end

The first set of eight axioms is that of a *commutative ring with* 1, which establishes the standard properties of $+$, $-$, and $\cdot$. We will refer to these axioms by $CR1, \ldots, CR8$.

equations *CR*

$$\begin{aligned}(x + y) + z &= x + (y + z)\\ x + y &= y + x\\ x + 0 &= x\\ x + (-x) &= 0\\ (x \cdot y) \cdot z &= x \cdot (y \cdot z)\\ x \cdot y &= y \cdot x\\ x \cdot 1 &= x\\ x \cdot (y + z) &= x \cdot y + x \cdot z\end{aligned}$$

end

Our first set *SIP* of axioms for $^{-1}$ contain the following, which we call the *strong inverse properties*. They are "strong" because they are equations involving $^{-1}$ *without any guards*, such as $x \neq 0$:

equations *SIP*

$$\begin{aligned}(-x)^{-1} &= -(x^{-1})\\ (x \cdot y)^{-1} &= x^{-1} \cdot y^{-1}\\ (x^{-1})^{-1} &= x\end{aligned}$$

end

We will refer to these axioms by $SIP1, \ldots, SIP3$. The set $CR \cup SIP$ of equations and its extensions are our basic object of study. We will also need other axioms, especially about $^{-1}$.

Later, we will add to $CR \cup SIP$ the *restricted inverse law* (*Ril*),

$$x \cdot (x \cdot x^{-1}) = x,$$

which, using commutativity and associativity, expresses that $x \cdot x^{-1}$ is 1 in the presence of x.

Hirschfeld (Personal Communication 2006) has shown that equations $SIP1$ and $SIP2$ are derivable from $SIP3$ using $CR \cup Ril$.

The standard axioms of a field simply add to *CR* the following: the *general inverse law* (*Gil*)

$$x \neq 0 \implies x \cdot x^{-1} = 1$$

and the *axiom of separation* (Sep)

$$0 \neq 1.$$

Guarded versions of the equations of *SIP*—such as, $x \neq 0 \implies (x^{-1})^{-1} = x$—can be proved from *Gil* and Sep.

2.3. TOTALIZED FIELDS AND ALGEBRAS SATISFYING THE SPECIFICATIONS. Let us consider the notion of a field in our setting. Let (Σ, T_{field}) be the axiomatic specification of fields, where

$$T_{field} = CR \cup Gil \cup Sep.$$

The class $Alg(\Sigma, T_{field})$ is the class of *total* algebras satisfying the axioms in T_{field}. For emphasis, we refer to these algebras as *totalized fields*.

For all totalized fields $A \in Alg(\Sigma, T_{field})$ and all $x \in A$, the inverse x^{-1} is defined. In particular, 0_A^{-1} is defined. What can it be?

Now suppose $0_A^{-1} = a$ for some $a \in A$. Then, we must expect that

$$0_A^{-1} \cdot 0_A \neq 1_A.$$

To see this, note that $a \cdot 0_A = 0_A$ for all a in a ring (see Lemma 2.1(a) below). So $0_A^{-1} \cdot 0_A = 0_A$ and $0_A \neq 1_A$ by Sep. Thus, at this stage, the actual value $0_A^{-1} = a$ can be anything. Choosing $0_A^{-1} = a$ we may speak of an *a-totalized field* and, in particular, when $a = 0$ of a 0-*totalized field*.

Now, the axiomatic theory of fields is one of the central topics in the model theory of first order languages: it has shaped the subject and led to its best applications. In model theory operations in signatures are invariably total. It is common to axiomatise fields using a set of Π_2 sentences over the ring signature thus avoiding the question of the totality of the inverse operation. However, with this ring signature, the substructures are rings and not necessarily fields. Thus, axiomatisations based on the field signature with the following axiom are also used (see, e.g., Hodges [1993, p. 695])

$$0^{-1} = 0 \wedge x \neq 0 \implies x \cdot x^{-1} = 1.$$

In fact, 0 is a common choice for the value of 0^{-1}. In automated reasoning, for example, Harrison [1998] used $0^{-1} = 0$ and observed that *SIP*1, *SIP*2 and *SIP*3 are valid in the 0-totalised reals.

Our own interest will be in the specification $CR \cup SIP$. Shortly, we shall show that this specification will force the choice of $0^{-1} = 0$.

The main Σ-algebra we are interested in is

$$Q_0 = (\mathbb{Q} \mid 0, 1, +, -, \cdot, ^{-1})$$

where the inverse is total

$$\begin{aligned} x^{-1} &= 1/x && \text{if } x \neq 0; \\ &= 0 && \text{if } x = 0. \end{aligned}$$

This total algebra satisfies the axioms of a field T_{field} and is a 0-totalized field of rationals.

Similarly, we can define the a-totalized field Q_a of rationals where the inverse is made total by $0^{-1} = a$.

2.4. PROPERTIES. We will now derive some simple equational properties from the axioms.

LEMMA 2.1. *The following equations are provable from CR:*
(a) $0 \cdot x = 0$.
(b) $(-1) \cdot x = -x$.
(c) $(-x) \cdot y = -(x \cdot y)$.
(d) $-0 = 0$.
(e) $(-x) + (-y) = -(x + y)$.
(f) $-(-x) = x$.

PROOF
(a) We calculate:

$$\begin{aligned}
0 + 0 &= 0 && \text{by } CR3\\
(0 + 0) \cdot x &= 0 \cdot x && \text{multiplying both sides by } x\\
0 \cdot x + 0 \cdot x &= 0 \cdot x && \text{by } CR8 \text{ and } CR6\\
(0 \cdot x + 0 \cdot x) + (-(0 \cdot x)) &= 0 \cdot x + (-(0 \cdot x)) && \text{adding to both sides}\\
0 \cdot x + (0 \cdot x + (-(0 \cdot x))) &= 0 && \text{by } CR1 \text{ and } CR4\\
0 \cdot x + 0 &= 0 && \text{by } CR4\\
0 \cdot x &= 0 && \text{by } CR3.
\end{aligned}$$

(b) We calculate:

$$\begin{aligned}
(-1) \cdot x &= (-1) \cdot x + (x - x) && \text{by } CR3 \text{ and } CR4\\
&= ((-1) \cdot x + (x \cdot 1)) - x && \text{by } CR7 \text{ and } CR1\\
&= ((-1) \cdot x + (1 \cdot x)) - x && \text{by } CR6\\
&= ((-1) + 1) \cdot x - x && \text{by } CR8\\
&= (1 + (-1)) \cdot x - x && \text{by } CR2\\
&= 0 \cdot x - x && \text{by } CR4\\
&= 0 - x && \text{by this Lemma clause (a)}\\
&= -x && \text{by } CR3.
\end{aligned}$$

(c) We calculate:

$$\begin{aligned}
(-x) \cdot y &= ((-1) \cdot x) \cdot y && \text{by this Lemma clause (b)}\\
&= (-1) \cdot (x \cdot y) && \text{by } CR5\\
&= -(x \cdot y) && \text{by this Lemma clause (b).}
\end{aligned}$$

(d) We calculate:

$$\begin{aligned}
-0 &= (-1) \cdot 0 && \text{by this Lemma clause (b)}\\
&= 0 && \text{by this Lemma clause (a).}
\end{aligned}$$

(e) We calculate:

$$\begin{aligned}
(-x)+(-y) &= 0+((-x)+(-y)) && \text{by } CR3\\
&= (-(x+y)+(x+y))+((-x)+(-y)) && \text{by } CR3\\
&= -(x+y)+((x+-x)+(y+-y)) && \text{by } CR1 \text{ and } CR2\\
&= -(x+y)+(0+0) && \text{by } CR4\\
&= -(x+y)+0 && \text{by } CR3\\
&= -(x+y) && \text{by } CR3.
\end{aligned}$$

(f) We calculate:

$$\begin{aligned}
-(-x) &= 0+-(-x) && \text{by } CR3\\
&= (x+(-x))+-(-x) && \text{by } CR4\\
&= x+((-x)+-(-x)) && \text{by } CR1\\
&= x+0 && \text{by } CR3\\
&= x && \text{by } CR3. \qquad \square
\end{aligned}$$

We know from (a) that $0 = 0 \cdot 0^{-1}$ is valid in a commutative ring. On adding the axioms *SIP* to *CR*, we force a value for 0^{-1}:

THEOREM 2.2. *The following equation is provable from CR* $\cup$ *SIP:*

$$0^{-1} = 0.$$

PROOF. First observe that:

$$\begin{aligned}
0 &= 0^{-1}+-(0^{-1}) && \text{by } CR4\\
&= 0^{-1}+(-0)^{-1} && \text{by } SIP1\\
&= 0^{-1}+0^{-1} && \text{by Lemma 2.1(d).}
\end{aligned}$$

Now we calculate:

$$\begin{aligned}
0^{-1} &= (0^{-1}+0^{-1})^{-1} && \text{by applying } {}^{-1}\\
&= (1\cdot 0^{-1}+1\cdot 0^{-1})^{-1} && \text{by } CR6 \text{ and } CR7\\
&= ((1+1)\cdot 0^{-1})^{-1} && \text{by } CR8\\
&= (1+1)^{-1}\cdot (0^{-1})^{-1} && \text{by } SIP2\\
&= (1+1)^{-1}\cdot 0 && \text{by } SIP3\\
&= 0 && \text{by Lemma 2.1(a) and } CR2. \qquad \square
\end{aligned}$$

2.5. EQUATIONAL SUBTHEORIES OF FIELDS. Given the three axioms of *SIP*, one might ask: What is wrong with the unguarded equation $x \cdot x^{-1} = 1$? It is easy to show that it contradicts *Sep*, that is,

$$CR \cup \{x \cdot x^{-1} = 1\} \vdash 0 = 1.$$

So we must try other equations for inverse. The axiom *Ril* implies a wider context for inverse.

LEMMA 2.3. $CR \cup SIP \cup Ril \vdash u \cdot x \cdot y = u \implies u \cdot x \cdot x^{-1} = u.$

PROOF. We calculate:

$$\begin{aligned} u \cdot x \cdot x^{-1} &= (u \cdot x \cdot y) \cdot x \cdot x^{-1} && \text{by premiss} \\ &= u \cdot y \cdot x \cdot x \cdot x^{-1} && \text{by commutativity} \\ &= u \cdot y \cdot x && \text{by } \mathit{Ril} \\ &= u && \text{by premiss.} \quad \square \end{aligned}$$

Let us show that the equational specifications are (almost) subtheories of $T_{\mathit{field}} = \mathit{CR} \cup \mathit{Gil} \cup \mathit{Sep}$. First, we need this cancelation lemma:

LEMMA 2.4. $T_{\mathit{field}} \vdash x \cdot y = 1 \wedge x \cdot z = 1 \rightarrow y = z$.

PROOF. If $x \cdot y = 1$, then $x \neq 0$. Multiply both assumptions by x^{-1} and we have $x^{-1} \cdot x \cdot y = x^{-1}$ and $x^{-1} \cdot x \cdot z = x^{-1}$. So, using *Gil* for $x \neq 0$, we have $1 \cdot y = x^{-1}$ and $1 \cdot z = x^{-1}$. By *CR*7, we have $y = x^{-1} = z$. $\square$

LEMMA 2.5. $T_{\mathit{field}} \cup \{0^{-1} = 0\} \vdash \mathit{SIP}$ *and* $T_{\mathit{field}} \cup \{0^{-1} = 0\} \vdash \mathit{Ril}$.

PROOF. Consider the three axioms of *SIP* in turn.

(1) $(-x)^{-1} = -(x^{-1})$. If $x = 0$, then the equation is true trivially. Suppose $x \neq 0$ and so $-x \neq 0$. We calculate:

$$\begin{aligned} 1 &= (-x) \cdot (-x)^{-1} && \text{by } \mathit{Gil} \\ &= (-1 \cdot x) \cdot (-x)^{-1} && \text{by Lemma 2.1(b)} \\ &= x \cdot -1 \cdot (-x)^{-1} && \text{by } \mathit{CR}6 \\ &= x \cdot -(-x)^{-1} && \text{by Lemma 2.1(b).} \end{aligned}$$

By *Gil*, we also have $1 = x \cdot x^{-1}$. So,

$$\begin{aligned} x^{-1} &= -(-x)^{-1} && \text{by Cancellation Lemma 2.4} \\ -(x^{-1}) &= -(-(-x)^{-1}) && \text{by applying } - \\ &= (-x)^{-1} && \text{by Lemma 2.1(f).} \end{aligned}$$

(2) $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$. If $x = 0$ or $y = 0$, then the equation is true trivially. If $x \neq 0$ and $y \neq 0$, then $x \cdot y \neq 0$. By *Gil*, we have

$$(x \cdot y) \cdot (x \cdot y)^{-1} = 1$$

and by the axioms of *CR*

$$(x \cdot y) \cdot x^{-1} \cdot y^{-1} = 1 \cdot 1 = 1.$$

Thus, by cancellation, $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$.

(3) $(x^{-1})^{-1} = x$. If $x = 0$, then the equation is true trivially. If $x \neq 0$, then $x^{-1} \neq 0$. By *Gil*, we have

$$(x^{-1}) \cdot (x^{-1})^{-1} = 1 \text{ and } (x^{-1}) \cdot x = 1.$$

By cancellation, $(x^{-1})^{-1} = x$.

The derivation of *Ril* is obvious. $\square$

Notice that for any closed equation, $T_{field} \vdash t = s$ implies $T_{field} \cup \{0^{-1} = 0\} \vdash t = s$, which is trivial as $\vdash$ is monotonic.

3. *Initial Algebra Specification*

We give two algebraic specifications of the rationals, one infinite and one finite.

3.1. A RECURSIVE EQUATIONAL SPECIFICATION. Let us define the numerals over Σ by $\underline{0} = 0$ and $\underline{n+1} = \underline{n} + 1$. We denote $0, 1, 1+1, (1+1)+1, \ldots$ by $0, \underline{1}, \underline{2}, \underline{3}, \ldots$. Now we define a set I of closed Σ-equations between numerals by

$$I = \{\underline{n} \cdot (\underline{n})^{-1} = 1 \mid n > 0\}.$$

THEOREM 3.1. *There exists a recursive equational initial algebra specification* $(\Sigma, CR \cup SIP \cup I)$*, without hidden functions, of the totalised field* Q_0 *of rational numbers, that is,*

$$T(\Sigma, CR \cup SIP \cup I) \cong Q_0.$$

PROOF. Clearly, the specification I is decidable. Note that, by inspection,

$$Q_0 \models CR \cup SIP \cup I.$$

By initiality, there exists a unique Σ-homomorphism $\phi\colon T(\Sigma, CR \cup SIP \cup I) \to Q_0$.

As Q_0 is Σ-minimal, we know that ϕ is surjective. Thus, to complete the proof, we must show that ϕ is also injective.

Consider Q_0. The domain $\mathbb{Q}$ of Q_0 can be represented as follows:

$$\begin{aligned}\mathbb{Q} = \{0\} &\cup \left\{\tfrac{n}{m} \mid n > 0, m > 0, gcd(n,m) = 1\right\} \\ &\cup \left\{-\tfrac{n}{m} \mid n > 0, m > 0, gcd(n,m) = 1\right\}.\end{aligned}$$

We use this representation to calculate the values of ϕ on certain equivalence classes of terms in $T(\Sigma, CR \cup SIP \cup I)$:

LEMMA 3.2. *The following hold:*
$\phi([\underline{0}]) = 0$
$\phi([\underline{1}]) = 1$
$\phi([\underline{n}]) = n$
$\phi([\underline{n}^{-1}]) = \frac{1}{n}$
$\phi([\underline{n} \cdot \underline{m}^{-1}]) = \frac{n}{m}$, *providing* $gcd(n,m) = 1$.
$\phi([-(\underline{n} \cdot \underline{m}^{-1})]) = -\frac{n}{m}$, *providing* $gcd(n,m) = 1$.

PROOF. Cases (i) and (ii) are obvious since ϕ preserves constants. Case (iii) is shown by induction on n. Case (iv) is shown by induction on n and uses the interpretation of $^{-1}$. The last two cases are based on

$$\phi([\underline{n} \cdot \underline{m}^{-1}]) = \begin{cases} \frac{\phi([\underline{n}])}{\phi([\underline{m}])} & \text{if } gcd(n,m) = 1; \\ \frac{n : gcd(n,m)}{m : gcd(n,m)} & \text{otherwise} \end{cases}$$

where we use: to denote division on natural numbers. □

These observations suggest the following definition and lemma. Let

$$TR = \{\underline{0}\} \cup \{\underline{n} \cdot \underline{m}^{-1} \mid n > 0, m > 0, gcd(n, m) = 1\} \\ \cup \{-(\underline{n} \cdot \underline{m}^{-1}) \mid n > 0, m > 0, gcd(n, m) = 1\}.$$

LEMMA 3.3. *The set TR is a transversal for the equivalence relation* $\equiv_{CR \cup SIP \cup I}$, *that is, each equivalence class contains one and only one element of TR.*

Before we prove Lemma 3.3, let us note that it is enough to prove ϕ is injective. For suppose

$$\phi([t]) = \phi([t']).$$

Then, by Lemma 3.3, we know that $[t] = [r]$ and $[t'] = [r']$ for unique $r, r' \in TR$. Thus,

$$\phi([r]) = \phi([r']).$$

But, by Lemma 3.2, we know that $\phi([r])$ and $\phi([r'])$ have values in the normal form of $\frac{n}{m}$, or $-\frac{n}{m}$, provided $gcd(n, m) = 1$, etc. This happens if, and only if, $r = r'$ and hence if, and only if, $[t] = [t']$.

It remains to prove the Lemma 3.3 as follows:

PROOF. Let $E = CR \cup SIP \cup I$. We have to show that:

(1) for each closed term $t \in T(\Sigma)$ there is some $u \in TR$ such that $E \vdash t = u$;
(2) for any closed terms $k, l \in TR$, if $E \vdash k = l$ then $k \equiv l$.

The proof of (1) is by induction on the structure of term t and requires a large case analysis based on the leading function symbol of t in Σ and possible normal forms for subterms in TR. We give one of the induction cases for illustration:

Case: Multiplication $t = r \cdot s$.

By induction, both r and s are provably equivalent to elements of TR. We take the following subcase: suppose

$$(\Sigma, E) \vdash r = \underline{n} \cdot \underline{m}^{-1} \text{ and } E \vdash s = -(\underline{k} \cdot \underline{l}^{-1}).$$

Now,

$$\begin{aligned}
(\Sigma, E) &\vdash r \cdot s = \underline{n} \cdot \underline{m}^{-1} \cdot -(\underline{k} \cdot \underline{l}^{-1}) && \text{by substitution} \\
&\vdash r \cdot s = \underline{n} \cdot \underline{m}^{-1} \cdot (-1) \cdot (\underline{k} \cdot \underline{l}^{-1}) && \text{by } CR6 \text{ and } CR7 \\
&\vdash r \cdot s = (-1) \cdot \underline{n} \cdot \underline{m}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1} && \text{by } CR8 \\
&\vdash r \cdot s = (-1) \cdot (\underline{n} \cdot \underline{k}) \cdot (\underline{m}^{-1} \cdot \underline{l}^{-1}) && \text{by } SIP2 \\
&\vdash r \cdot s = (-1) \cdot (\underline{n} \cdot \underline{k}) \cdot (\underline{m} \cdot \underline{l})^{-1} && \text{by } SIP3 \\
&\vdash r \cdot s = (-1) \cdot (\underline{n.k}) \cdot (\underline{m.l})^{-1} && \text{by } SIP3 \\
&\vdash r \cdot s = -(\underline{n.k}) \cdot (\underline{m.l})^{-1} && \text{by } SIP3.
\end{aligned}$$

Now let $u = gcd(n.k, m.l)$. If $u = 1$, then we are done. Suppose that $n.k = u.p$ and $m.l = u.q$ and so $gcd(p, q) = 1$. Then we continue rewriting:

$$\begin{aligned}
(\Sigma, E) &\vdash r \cdot s = -(\underline{u.p}) \cdot (\underline{u.q})^{-1} && \text{by definition}\\
&\vdash r \cdot s = -(\underline{u} \cdot \underline{p}) \cdot (\underline{u} \cdot \underline{q})^{-1} && \text{by Lemma 3.4}\\
&\vdash r \cdot s = -(\underline{u} \cdot \underline{u}^{-1})(\underline{p} \cdot \underline{q}^{-1}) && \text{by } CR6 \text{ and } SIP2\\
&\vdash r \cdot s = -\underline{p} \cdot \underline{q}^{-1} && \text{by equations of I.}
\end{aligned}$$

The term $-\underline{p} \cdot \underline{q}^{-1}$ is of the required form because $gcd(p, q) = 1$. The following is an easy induction.

LEMMA 3.4. *For any $p, q \in \mathbb{N}$ we have*

$$\begin{aligned}
(\Sigma, E) &\vdash \underline{p + q} = \underline{p} + \underline{q}\\
(\Sigma, E) &\vdash \underline{p.q} = \underline{p} \cdot \underline{q}\\
(\Sigma, E) &\vdash \underline{-p} = -\underline{p}.
\end{aligned}$$

The proof of uniqueness condition (2) is easy: Suppose $k \neq l$. Then they have different interpretations in Q_0 under ϕ. This means that they cannot be proved equal by the axioms $CR \cup SIP \cup I$ since Q_0 satisfies these axioms.

This completes the proof of Lemma 3.3 and hence the proof of Theorem 3.1. □

3.2. A FINITE EQUATIONAL SPECIFICATION. We first introduce an operation:

Definition 3.5. $Z(x) = 1 - x \cdot x^{-1}$.

The operator "measures" the difference between $x \cdot x^{-1}$ and 1. Clearly,

$$Z(x) = 0 \Leftrightarrow x \cdot x^{-1} = 1.$$

The operator has many useful properties. For example, the set I of closed equations used in Section 3.1 can be written

$$I = \{Z(\underline{n}) = 0 \mid n > 0\}.$$

The operator Z is a function that is definable by a term over the field signature. It is used to simplify notations and calculations below. It does not count as a hidden function as it can be simply removed from all specifications by expanding its explicit definition.

Recall *Lagrange's Theorem* that every natural number can be represented as the sum of four squares (see Dickson [1952, pp. 275–303]). We define a special equation L (for Lagrange):

$$Z(1 + x^2 + y^2 + z^2 + u^2) = 0.$$

L expresses that for a large collection of numbers (in particular, those q which can be written as 1 plus the sum of four squares) $q \cdot q^{-1}$ equals 1.

THEOREM 3.6. *There exists a finite equational initial algebra specification, without hidden functions, of the totalised field Q_0 of rational numbers; in particular,*

$$T(\Sigma, CR \cup SIP \cup L) \cong Q_0.$$

PROOF. First, note that, by inspection,

$$Q_0 \models CR \cup SIP \cup L.$$

We know that *CR* and *SIP* are valid in Q_0. To see that L is valid, note that $(1 + x^2 + y^2 + z^2 + w^2)$ is always positive and never 0. Since $Q_0 \models x \neq 0 \implies x \cdot x^{-1} = 1$, we conclude that L is valid.

By initiality, there exists a unique Σ-homomorphism $\phi\colon T(\Sigma, CR \cup SIP \cup L) \to Q_0$.

As Q_0 is Σ-minimal, we know that ϕ is surjective. Thus, to complete the proof, we must show that ϕ is also injective.

On the other hand, recalling the recursive set I of numerals Section 3.1, we know that

$$L \vdash I.$$

This is because for each $n \in \mathbb{N}$ we can choose some x, y, z, w such that $n = 1 + x^2 + y^2 + z^2 + w^2$. Therefore,

$$T(\Sigma, CR \cup SIP \cup L) \models CR \cup SIP \cup I.$$

By initiality, there exists a unique Σ-homomorphism $\phi\colon T(\Sigma, CR \cup SIP \cup I) \to T(\Sigma, CR \cup SIP \cup L)$. But, by Theorem 3.1, $T(\Sigma, CR \cup SIP \cup I) \cong Q_0$ and so there is a Σ-homomorphism $\psi\colon Q_0 \to T(\Sigma, CR \cup SIP \cup L)$. Thus, by minimality, we have ϕ is a Σ-isomorphism with ψ as its inverse and $T(\Sigma, CR \cup SIP \cup L) \cong Q_0$. □

4. *A Simpler Specification using the Modulus Function*

Consider the algebra Q_0 of rational numbers expanded with the modulus function $|\,|$ and let this be denoted

$$Q_{0,||} = (\mathbb{Q} \mid 0, 1, +, -, \cdot, ^{-1}, |\,|).$$

We will give an equational specification of this algebra. The following two sets of equations can be added to $CR \cup SIP$. The first specifies the modulus operator on the rational numbers.

equations *MOD*

$$\begin{aligned} |0| &= 0 \\ |1| &= 1 \\ |-x| &= |x| \\ |x \cdot y| &= |x| \cdot |y| \\ |x^{-1}| &= (|x|)^{-1} \\ |1 + (|x|)| &= 1 + |x| \end{aligned}$$

end

The second guarantees the existence of proper inverses for sufficiently many closed terms.

equations *Modril*

$$Z(1 + |x|) = 0$$

end

To get used to the axioms for $|\ |$, we prove a simple lemma of use later:

LEMMA 4.1. *For each $k \in \mathbb{N}$, $CR \cup MOD \vdash |\underline{k}| = \underline{k}$.*

PROOF. By induction on k.

Basis, $k = 0$: We calculate:

$\|\underline{0}\| = \|0\|$	by definition of $\underline{0}$
$= 0$	by $MOD1$
$= \underline{0}$	by definition of $\underline{0}$.

Induction step, $k+1$, Assume as induction hypothesis that $|\underline{k}| = \underline{k}$. We calculate:

$\underline{k+1} = \underline{k} + 1$	by definition of $\underline{k+1}$
$= 1 + \underline{k}$	by commutativity $CR2$
$= 1 + \|\underline{k}\|$	by induction hypothesis
$= \|1 + \|\underline{k}\|\|$	by $MOD6$
$= \|1 + \underline{k}\|$	by induction hypothesis
$= \|\underline{k+1}\|$	by $CR2$ and the definition of $\underline{k+1}$.

□

THEOREM 4.2. *The initial algebra $T(\Sigma \cup \{||\}, CR \cup SIP \cup MOD \cup Modril)$ is isomorphic to the algebra $Q_{0,||}$ of rational numbers.*

PROOF. The proof follows the pattern of earlier theorems (Theorems 3.1 and 3.6). For notational convenience, let

$$E = CR \cup SIP \cup MOD \cup Modril.$$

The equations in E are valid in $Q_{0,||}$. Thus, by initiality, there exists a unique $\Sigma \cup \{|\ |\}$-homomorphism

$$\psi : T(\Sigma \cup \{|\ |\}, E) \to Q_{0,||}.$$

As $Q_{0,||}$ is $\Sigma \cup \{|\ |\}$-minimal, we know that ψ is surjective. Thus, to complete the proof, we must show that ψ is also injective.

The carrier of $Q_{0,||}$ is the same as Q_0 and is

$$\begin{aligned}\mathbb{Q} = \{0\} &\cup \left\{\tfrac{n}{m} \mid n > 0, m > 0, gcd(n,m) = 1\right\} \\ &\cup \left\{-\tfrac{n}{m} \mid n > 0, m > 0, gcd(n,m) = 1\right\}.\end{aligned}$$

This suggests that we should use the previous transversal

$$\begin{aligned}TR = \{\underline{0}\} &\cup \{\underline{n} \cdot \underline{m}^{-1} \mid n > 0, m > 0, gcd(n,m) = 1\} \\ &\cup \{-(\underline{n} \cdot \underline{m}^{-1}) \mid n > 0, m > 0, gcd(n,m) = 1\}.\end{aligned}$$

as a transversal for $T(\Sigma \cup \{|\ |\}, E)$. Following the pattern of Theorem 3.1, we can prove new versions of the evaluation and transversal Lemmas 3.2 and 3.3.

First, we generalize the numeral notation for the naturals to a notation for the rationals. For each $r \in \mathbb{Q}$, we define

$$\begin{aligned} \underline{r} &= 0 && \text{if } r = 0; \\ &= \underline{n} \cdot \underline{m}^{-1} && \text{if } r = \frac{n}{m} \text{ and } n > 0, m > 0, gcd(n, m) = 1 \\ &= -(\underline{n} \cdot \underline{m}^{-1}) && \text{if } r = -\frac{n}{m} \text{ and } n > 0, m > 0, gcd(n, m) = 1 \end{aligned}$$

Thus, with this notation, $TR = \{\underline{r} \mid r \in \mathbb{Q}\}$.

LEMMA 4.3. *The $\Sigma \cup \{|\,|\}$ homomorphism ψ satisfies $\psi([\underline{r}]) = r$ for all $r \in \mathbb{Q}$.*

PROOF. This follows the same arguments as the proof of Lemma 3.2. Note clauses (i), (v) and (vi). □

LEMMA 4.4. *The set TR is a transversal for the equivalence relation $\equiv_E$ on $T(\Sigma \cup \{|\,|\})$.*

Suppose we have proved this fact, then we can conclude the proof of the theorem as follows. If

$$\psi([t]) = \psi([t']),$$

then, by Lemma 4.4, there exist $\underline{r}, \underline{r}' \in TR$ such that

$$E \vdash t = \underline{r} \text{ and } E \vdash t' = \underline{r}'.$$

Thus,

$$\psi([\underline{r}]) = \psi([\underline{r}']).$$

Now, by Lemma 4.3,

$$\psi([\underline{r}]) = r \text{ and } \psi([\underline{r}']) = r'.$$

Thus,

$$r = r'.$$

Since *TR* is a transveral, this happens if, and only if, the terms

$$\underline{r} = \underline{r}'$$

and hence $[\underline{r}] = [\underline{r}']$ and $[\underline{t}] = [\underline{t}']$.

It remains to prove Lemma 4.4. We note the following.

LEMMA 4.5. $CR \cup MOD \cup Modril \vdash I$

PROOF. We can write the set I as

$$I = \{Z(\underline{n}) = 0 \mid n > 0\}$$

and so prove, by induction on $n > 0$, that $CR \cup MOD \cup Modril \vdash Z(\underline{n}) = 0$.

Basis $n = 1$. We calculate:

$$\begin{aligned} Z(\underline{1}) &= Z(\underline{1} + \underline{0}) && \text{by } CR3 \text{ and the definition of } \underline{0} \\ &= Z(\underline{1} + |\underline{0}|) && \text{by } MOD1 \\ &= 0 && \text{by } Modril. \end{aligned}$$

Induction Step $n = k + 1$. We calculate:

$$\begin{aligned} Z(\underline{k+1}) &= Z(\underline{k} + 1) && \text{by the definition of } \underline{k+1} \\ &= Z(1 + \underline{k}) && \text{by } CR2 \\ &= Z(1 + |\underline{k}|) && \text{by Lemma 4.1} \\ &= 0 && \text{by } Modril. \end{aligned}$$ □

We can show that for every term $t \in T(\Sigma \cup \{|\,|\})$ there is an $\underline{r} \in TR$ such that $E \vdash t = \underline{r}$. Notice that by Lemma 4.5, and Lemma 3.3, we know that for all terms t not containing $|\,|$, $t \in T(\Sigma)$, $E \vdash t = \underline{r}$.

We prove the transversal lemma by induction on the height $Ht(t)$ of terms $t \in T(\Sigma \cup \{|\,|\})$.

Basis. $Ht(t) = 0$. Then $t = 0$ or $t = 1$ and we are done.

Induction Step, $Ht(t) = k + 1$. Suppose that the lemma is true for terms of height lower than $Ht(t) = k$ and consider a term of height k. There are five cases corresponding to the operations. We consider two for illustration.

Case $t = s + s'$. By induction,

$$E \vdash s = \underline{r} \text{ and } E \vdash s' = \underline{r}'$$

for $\underline{r}, \underline{r}' \in TR$. Thus,

$$E \vdash s + s' = \underline{r} + \underline{r}'.$$

Now $\underline{r} + \underline{r}'$ does not contain $|\,|$ and so reduces to some element in TR.

Case $t = |s|$. This is the interesting case. By induction, $E \vdash s = \underline{r}$. There are three subcases.

If $\underline{r} = \underline{0}$, then $t = |\underline{r}| = |\underline{0}| = 0$ by $MOD1$.

If $\underline{r} = \underline{n} \cdot \underline{m}^{-1}$, then

$$\begin{aligned} t &= |\underline{n} \cdot \underline{m}^{-1}| && \text{by definition} \\ &= |\underline{n}| \cdot |\underline{m}^{-1}| && \text{by } MOD4 \\ &= |\underline{n}| \cdot |\underline{m}|^{-1} && \text{by } MOD5 \\ &= \underline{n} \cdot \underline{m}^{-1} && \text{by Lemma 4.1.} \end{aligned}$$

If $\underline{r} = -(\underline{n} \cdot \underline{m}^{-1})$, then

$$\begin{aligned} t &= |-(\underline{n} \cdot \underline{m}^{-1})| && \text{by the definition} \\ &= \underline{n} \cdot \underline{m}^{-1} && \text{by } MOD3. \end{aligned}$$ □

The specification $CR \cup SIP \cup MOD \cup Modril$ of the rational numbers is simpler than the specification $CR \cup SIP \cup L$ because it does not depend on (somewhat) sophisticated number theory.

5. *Specifications of Totalized Fields and Other Rational Arithmetics*

5.1. ON THE EQUATIONAL THEORY OF TOTALIZED FIELDS. It has long been known that the class of totalised fields is not a variety, that is, is not definable by equations over the field signature. The argument is based on the fact that the class of totalised fields is not closed under products (compare Birkhoff's Theorem, see, e.g., Meinke and Tucker [1992]).

We can rephrase and reprove this elementary fact in the present setting as follows:

LEMMA 5.1. *There is no set E of equations over the signature Σ of fields that is logically equivalent with $CR \cup SIP \cup Sep \cup Gil$.*

PROOF. Assume the contrary and suppose that there is such a set of equations E such that $Alg(\Sigma, E) = Alg(\Sigma, CR \cup SIP \cup Sep \cup Gil)$. Consider the initial algebra $I(\Sigma, E)$ of E. Now because the Σ-algebra Q_0 of rational numbers is a model of E, we know that

$$I(\Sigma, E) \models \neg(1 + 1 = 0).$$

To see this, note that if $1 + 1 = 0$ was valid in the initial model $I(\Sigma, E)$ in then it would be valid under every homomorphism and, in particular, would be valid in Q_0, which it is not.

Now, by assumption, $I(\Sigma, E) \models CR \cup SIP \cup Sep \cup Gil$ and this implies

$$I(\Sigma, E) \models Z(1 + 1) = 0.$$

But the prime totalized field Z_2 of characteristic 2 is also a model of $CR \cup SIP \cup Sep \cup Gil$. By initiality, here is an unique homomorphism $\phi : I(\Sigma, E) \to Z_2$ and, being a minimal structure, Z_2 must be a homomorphic image of $I(\Sigma, E)$. Now since $Z(x)$ is a term, $\phi Z(a) = Z(\phi(a))$ for all $a \in A$ and $\phi(Z(1 + 1)) = Z(\phi(1 + 1)) = Z(\phi(1) + \phi(1)) = Z(1 + 1)$. In Z_2, we have $1 + 1 = 0$, which implies $Z(1 + 1) = 1$. Thus, the unique homomorphism ϕ maps $Z(1 + 1) = 0$ in $I(\Sigma, E)$ to $Z(1 + 1) = 1$ in Z_2, which is impossible for a homomorphism since the algebras satisfy Sep. (In fact, more generally all homomorphisms between fields must be injective.) This is a contradiction. □

Using a similar argument one can prove that *there is no conditional equational theory CE over the signature Σ of fields which is equivalent to $CR \cup SIP \cup Sep \cup Gil$ in first order logic*.

5.2. THE RESTRICTED INVERSE LAW. Recall *Ril* is

$$x \cdot (x \cdot x^{-1}) = x.$$

In the presence of $CR \cup SIP$, another way of writing *Ril* is as follows:

$$Z(x) \cdot x = 0.$$

We will now use the equational specification $(\Sigma, CR \cup SIP \cup Ril)$. If one restricts attention to the closed equations over Σ, an interesting positive result is found (Theorem 5.6).

Now *Ril* is derivable from $CR \cup SIP \cup Sep \cup Gil$ and for that reason $CR \cup SIP \cup Ril$ is a weaker theory than $CR \cup SIP \cup Sep \cup Gil$. Of course, the key point is that $CR \cup SIP \cup Ril$ is an equational theory over Σ in which inverses are possible.

To illustrate further the implications of *Ril*, here is a listing of identities that can easily be proved from $CR \cup SIP \cup Ril$:

LEMMA 5.2. *The following equations can be proved from* $CR \cup SIP \cup Ril$

$$\begin{aligned} Z(0) &= 1 \\ Z(1) &= 0 \\ Z(x) \cdot Z(x) &= Z(x) \\ (Z(x))^{-1} &= Z(x) \\ (1 - Z(x)) \cdot (1 - Z(x)) &= 1 - Z(x) \\ (1 - Z(x))^{-1} &= 1 - Z(x). \end{aligned}$$

PROOF. Equations (1) and (2) are obvious in any commutative ring. The other cases are calculations; we do the remaining cases.

Consider $Z(x) \cdot Z(x) = Z(x)$.

$$\begin{aligned} Z(x) \cdot Z(x) &= (1 - x \cdot x^{-1}) \cdot (1 - x \cdot x^{-1}) \\ &= 1 - x \cdot x^{-1} - x \cdot x^{-1} + (x \cdot x^{-1}) \cdot (x \cdot x^{-1}) \\ &= 1 - x \cdot x^{-1} - x \cdot x^{-1} + (x \cdot x^{-1} \cdot x) \cdot x^{-1} \\ &= 1 - x \cdot x^{-1} - x \cdot x^{-1} + x \cdot x^{-1} && \text{by } Ril \\ &= 1 - x \cdot x^{-1} \\ &= Z(x). \end{aligned}$$

Consider $Z(x)^{-1} = Z(x)$.

$$\begin{aligned} Z(x)^{-1} &= Z(x)^{-1} \cdot (Z(x)^{-1} \cdot Z(x)) && \text{by } Ril \\ &= (Z(x) \cdot Z(x))^{-1} \cdot Z(x) && \text{by } SIP \\ &= Z(x)^{-1} \cdot Z(x) && \text{by above} \\ &= Z(x)^{-1} \cdot Z(x) \cdot Z(x) && \text{by above} \\ &= Z(x). \end{aligned}$$

Consider $(1 - Z(x)) \cdot (1 - Z(x)) = 1 - Z(x)$.

$$\begin{aligned} (1 - Z(x)) \cdot (1 - Z(x)) &= 1 - Z(x) - Z(x) + Z(x) \cdot Z(x) && \text{by expansion} \\ &= 1 - Z(x) - Z(x) + Z(x) && \text{by above} \\ &= 1 - Z(x). \end{aligned}$$

Consider $(1 - Z(x))^{-1} = 1 - Z(x)$.

$$\begin{aligned}
(1 - Z(x))^{-1} &= (1 - (1 - x \cdot x^{-1}))^{-1} && \text{by expansion}\\
&= (x \cdot x^{-1})^{-1}\\
&= x^{-1} \cdot (x^{-1})^{-1} && \text{by } CR\\
&= x^{-1} \cdot x && \text{by } CR\\
&= x \cdot x^{-1}\\
&= (1 - (1 - x \cdot x^{-1}))\\
&= 1 - Z(x).
\end{aligned}$$

□

LEMMA 5.3. *Let p, q be different prime numbers. Then*

$$CR \cup SIP \cup Ril \vdash Z(\underline{p}) \cdot Z(\underline{q}) = 0.$$

PROOF. Let $a, b \in \mathbb{Z}$ be such that $1 = a \cdot p + b \cdot q$. There are different cases of which we will do one. Assume $a = n$ and $b = -m$ for $n, m \in \mathbb{N}$. Then $\underline{1} = \underline{n} \cdot \underline{p} - \underline{m} \cdot \underline{q}$. We calculate:

$$\begin{aligned}
Z(\underline{p}) &= Z(\underline{p}) \cdot 1 && \text{by multiplying}\\
&= Z(\underline{p}) \cdot (\underline{n} \cdot \underline{p} - \underline{m} \cdot \underline{q}) && \text{by substituting}\\
&= Z(\underline{p}) \cdot \underline{n} \cdot \underline{p} - Z(\underline{p}) \cdot \underline{m} \cdot \underline{q} && \text{by } SIP\\
&= Z(\underline{p}) \cdot \underline{p} \cdot \underline{n} - Z(\underline{p}) \cdot \underline{q} \cdot \underline{m} && \text{by above}\\
&= 0 \cdot \underline{n} - Z(\underline{p}) \cdot \underline{q} \cdot \underline{m} && \text{by } Ril\\
&= Z(\underline{p}) \cdot \underline{q} \cdot -\underline{m}.
\end{aligned}$$

By Lemma 2.3, we have $Z(\underline{p}) = Z(\underline{p}) \cdot \underline{q} \cdot \underline{q}^{-1}$. Thus, $Z(\underline{p}) \cdot (1 - \underline{q} \cdot \underline{q}^{-1}) = 0$ and this is $Z(\underline{p}) \cdot Z(\underline{q}) = 0$.

LEMMA 5.4. *For each prime p and closed term $t \in \Sigma$, there is a unique natural number $n < p$ such that*

$$CR \cup SIP \cup Ril \vdash Z(\underline{p}) \cdot t = Z(\underline{p}) \cdot \underline{n}.$$

PROOF. This is proved by an induction on the structure of t.

Basis. If $t \equiv \underline{k}$ then write $k = n + p \cdot l$ for natural numbers n and l with $n < p$. Now

$$\begin{aligned}
Z(\underline{p}) \cdot \underline{k} &= Z(\underline{p}) \cdot \underline{n + p \cdot l} && \text{by substitution}\\
&= Z(\underline{p}) \cdot \underline{n} + Z(\underline{p}) \cdot \underline{p} \cdot \underline{l} && \text{by } CR\\
&= Z(\underline{p}) \cdot \underline{n} && \text{by } Ril.
\end{aligned}$$

Induction Step. There are four cases corresponding with $+, -, \cdot, ^{-1}$ of which we will do one for illustration.

Let $t \equiv r^{-1}$ then we calculate:

$$\begin{aligned}
Z(\underline{p}) \cdot \underline{t} &= Z(\underline{p}) \cdot r^{-1} && \text{by substitution}\\
&= Z(\underline{p}) \cdot Z(\underline{p}) \cdot r^{-1} && \text{by Lemma 5.2}\\
&= Z(\underline{p}) \cdot (Z(\underline{p}))^{-1} \cdot r^{-1} && \text{by Lemma 5.2}\\
&= Z(\underline{p}) \cdot (Z(\underline{p}) \cdot r)^{-1} && \text{by } \mathit{SIP}\\
&= Z(\underline{p}) \cdot (Z(\underline{p}) \cdot \underline{n})^{-1} && \text{by induction}\\
&= Z(\underline{p}) \cdot (Z(\underline{p}))^{-1} \cdot \underline{n}^{-1} && \text{by } \mathit{SIP}\\
&= Z(\underline{p}) \cdot \underline{n}^{-1} && \text{by Lemma 5.2}\\
&= Z(\underline{p}) \cdot \underline{m} && \text{with } m < p \text{ such that } m = n^{-1} \mod p.
\end{aligned}$$

That the number $\underline{n}$ is unique follows from an inspection of the prime field of characteristic p. In that field $Z(\underline{p})$ equals 1 while different numerals $\underline{n_1}$ and $\underline{n_2}$ with n_1 and n_2 both below p have different interpretations.

By inspection, we can check the following refinement of the statement of the lemma.

COROLLARY 5.5. *Let $val_p^0(t)$ the value of term t in the totalised field K_p^0. The unique number $\underline{n}$ is $\underline{val_p^0(t)}$. Therefore, we have*

$$CR \cup SIP \cup Ril \vdash Z(\underline{p}) \cdot t = Z(\underline{p}) \cdot \underline{val_p^0(t)}.$$

The following theorem states that the equational subtheory T_{field}^0 can prove all the closed identities that are true in all fields.

THEOREM 5.6. *For any closed terms $t, t' \in T(\Sigma)$, we have*

$$T_{field}^0 \vdash t = t' \text{ implies } CR \cup SIP \cup Ril \vdash t = t'$$

Recall that if $T_{field} \vdash t = t'$ then $T_{field}^0 \vdash t = t'$.

PROOF. The proof is rather involved with many calculations needed to establish canonical forms. The canonical forms depend on the characteristics of the totalized fields.

Let p_n represent an enumeration of the primes in increasing order, starting with $p_0 = 2$. Then, we define the following special terms:

$$G_1 = 1, G_2 = 1 - Z(\underline{p_1}), G_{n+1} = G_n \cdot (1 - Z(\underline{p_n})).$$

For each n, the term G_n equals 0 in any prime field $K_{p_n}^0$ with characteristic p_n or less. For all n, the term G_n equals 1 in any field of characteristic 0 and, in particular, in the totalized field of rational numbers.

LEMMA 5.7. *For all n, we have:*
(i) $G_n = 1 - Z(\underline{p_1}) - \cdots - Z(\underline{p_{n-1}})$.
(ii) $G_n \cdot Z(\underline{p_n}) = Z(\underline{p_n})$
(iii) if $n \leq m$, *then* $G_m \cdot G_n = G_m$
(iv) if $k < p_n$, *then* $G_n \cdot \underline{k} \cdot \underline{k}^{-1} = G_n$.

PROOF. Exercise.

Using these G terms the following lemma can be stated:

LEMMA 5.8. *For each closed term t over Σ, there is a unique term $\underline{r} \in TR$ such that $CR \cup SIP \cup Ril \vdash G_n \cdot t = G_n \cdot \underline{r}$.*

PROOF. The proof uses induction of the structure of terms. We give the case of addition in the induction step. Let $t \equiv r + s$ and assume that

$$CR \cup SIP \cup Ril \vdash G_n \cdot r = G_n \cdot r' \text{ and } CR \cup SIP \cup Ril \vdash G_m \cdot s = G_m \cdot s'$$

with $r', s' \in TR$. Now there is a case distinction on the possible forms of r' and s'.

Let $r' \equiv \underline{k} \cdot \underline{l}^{-1}$ and $s' \equiv \underline{u} \cdot \underline{v}^{-1}$. Take i larger than m and n such that p_i exceeds both l and v. Now $CR \cup SIP \cup Ril$ proves

$$\begin{aligned}
G_i \cdot t = G_i \cdot (r + s) &= G_i \cdot r + G_i \cdot s \\
&= G_i \cdot \underline{k} \cdot \underline{l}^{-1} + G_i \cdot \underline{u} \cdot \underline{v}^{-1} \\
&= G_i \cdot \underline{v} \cdot \underline{v}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1} + G_i \cdot \underline{l} \cdot \underline{l}^{-1} \cdot \underline{u} \cdot \underline{v}^{-1} \\
&= G_i \cdot (\underline{v} \cdot \underline{k} \cdot \underline{v}^{-1} \cdot \underline{l}^{-1} + \underline{l} \cdot \underline{u} \cdot \underline{l}^{-1} \cdot \underline{v}^{-1}) \\
&= G_i \cdot (\underline{v} \cdot \underline{k} + \underline{l} \cdot \underline{u}) \cdot (\underline{l} \cdot \underline{v})^{-1} \\
&= G_i \cdot \underline{v \cdot k + l \cdot u} \cdot (\underline{l \cdot v})^{-1} \\
&= G_i \cdot \underline{k'} \cdot (\underline{l'})^{-1}.
\end{aligned}$$

If k' and l' are not relatively prime, they share a prime factor $q = p_j$. In particular: $k' = q \cdot k''$ and $l' = q \cdot l''$. Let $h = \max(i, j)$ then $CR \cup SIP \cup Ril \vdash G_{i'} \cdot t = G_{i'} \cdot \underline{k''} \cdot \underline{l''}$. By repeating the removal of shared prime factors until no more exist the required representation is obtained. That the representation is unique follows from its interpretation in the prime field of characteristic 0. □

The following defines the canonical terms:

LEMMA 5.9. *Let $t \in T(\Sigma)$. Suppose that*

$$CR \cup SIP \cup Ril \vdash G_n \cdot t = G_n \cdot \underline{val_0^0(t)}.$$

Then, for all $m > n$,

$$CR \cup SIP \cup Ril \vdash t = \textstyle\sum_{i=1}^{m-1} Z(\underline{p_i}) \cdot \underline{val_{p_i}^0(t)} + G_m \cdot \underline{val_0^0(t)}.$$

PROOF. We begin with a lemma.

LEMMA 5.10. *For each $n \in \mathbb{N}$,*

$$CR \cup SIP \cup Ril \vdash G_n \cdot t = Z(\underline{p_n}) \cdot \underline{val_{p_n}^0(t)} + G_{n+1} \cdot t.$$

PROOF. This is a calculation:

$$\begin{aligned}
G_n \cdot t &= (Z(\underline{p_n}) + (1 - Z(\underline{p_n}))) \cdot G_n \cdot t && \text{by } CR \\
&= Z(\underline{p_n}) \cdot G_n \cdot t + (1 - Z(\underline{p_n})) \cdot G_n \cdot t && \text{by } CR \\
&= Z(\underline{p_n}) \cdot G_n \cdot t + G_{n+1} \cdot t && \text{by definition} \\
&= G_n \cdot Z(\underline{p_n}) \cdot t + G_{n+1} \cdot t && \text{by } CR \\
&= G_n \cdot Z(\underline{p_n}) \cdot \underline{val^0_{p_n}(t)} + G_{n+1} \cdot t && \text{by Corollary 5.5} \\
&= Z(\underline{p_n}) \cdot \underline{val^0_{p_n}(t)} + G_{n+1} \cdot t && \text{by Lemma 5.7.} \quad \square
\end{aligned}$$

Now we choose $k \in \mathbb{N}$ such that $CR \cup SIP \cup Ril \vdash G_k \cdot t = G_k \cdot \underline{r}$ for some $\underline{r} \in TR$. Then we may expand the formula as follows:

$$\begin{aligned}
t &= G_1 \cdot t && \text{because } G_1 = 1 \text{ and } CR \\
&= Z(\underline{p_1}) \cdot \underline{val^0_{p_1}(t)} + G_2 \cdot t && \text{by Lemma 5.10} \\
&= Z(\underline{p_1}) \cdot \underline{val^0_{p_1}(t)} + Z(\underline{p_2}) \cdot \underline{val^0_{p_2}(t)} + G_3 \cdot t && \text{by Lemma 5.10} \\
&= Z(\underline{p_1}) \cdot \underline{val^0_{p_1}(t)} + \cdots + Z(\underline{p_{k-1}}) \cdot \underline{val^0_{p_{k-1}}(t)} + G_k \cdot t && \text{by repeated use of Lemma 5.10} \\
&= Z(\underline{p_1}) \cdot \underline{val^0_{p_1}(t)} + \cdots + Z(\underline{p_{k-1}}) \cdot \underline{val^0_{p_{k-1}}(t)} + G_k \cdot \underline{r} && \text{by choice of } k.
\end{aligned}$$

This completes the proof of the Lemma 5.9 □

Finally, we can complete the proof of Theorem 5.6. Assume that

$$T^0_{field} \vdash t = s$$

for any closed terms $t, s \in T(\Sigma)$. We choose n, m such that

$$\begin{aligned}
CR \cup SIP \cup Ril \vdash G_n \cdot t = G_n \cdot \underline{val^0_0(t)} \\
CR \cup SIP \cup Ril \vdash G_m \cdot s = G_m \cdot \underline{val^0_0(s)}.
\end{aligned}$$

Take $k = max(n, m)$. Then, by Canonical Term Lemma 5.9,

$$\begin{aligned}
CR \cup SIP \cup Ril \vdash t = \textstyle\sum_{i=1}^{k} Z(\underline{p_i}) \cdot \underline{val^0_{p_i}(t)} + G_k \cdot \underline{val^0_0(t)} \\
CR \cup SIP \cup Ril \vdash s = \textstyle\sum_{i=1}^{k} Z(\underline{p_i}) \cdot \underline{val^0_{p_i}(s)} + G_k \cdot \underline{val^0_0(s)}.
\end{aligned}$$

Since $T^0_{field} \vdash t = s$, the values of these closed terms in all prime fields are identical, that is, for all p_i, $val^0_{p_i}(t) = val^0_{p_i}(s)$ and $val^0_0(t) = val^0_0(s)$. Thus, the expansions on the right-hand side are identical and so we have

$$CR \cup SIP \cup Ril \vdash t = s. \quad \square$$

The initial algebra of CR is the integers. However, we note that

COROLLARY 5.11. *The initial algebra of $CR \cup SIP \cup Ril$ is a computable algebra but it is not an integral domain.*

PROOF. It is easy to check that the completeness proof for closed term equations (Theorem 5.6) also provides the decidability of their derivability. In any integral domain, we have $x \cdot y = 0$ implies $x = 0$ or $y = 0$. Let $x = Z(2)$ and let $y = 1 - Z(2)$. We calculate: $CR \cup SIP \cup \vdash \mathsf{Z}(\mathsf{2}) \cdot (\mathsf{1} - \mathsf{Z}(\mathsf{2})) = \mathsf{Z}(\mathsf{2}) - \mathsf{Z}(\mathsf{2}) \cdot \mathsf{Z}(\mathsf{2}) = \mathsf{Z}(\mathsf{2}) - \mathsf{Z}(\mathsf{2}) = \mathsf{0}$. Thus, for these choices, $x \cdot y = 0$ in the initial meadow. But both x and y are not equal to 0 in the initial meadow because, under homomorphisms, $x \neq 0$ and $y \neq 0$ in prime fields with different characteristics 2 and 0.

The algebras that are models of $CR \cup SIP \cup Ril$ have nice properties, in spite of not being fields nor even integral domains. We have the following proposal for a name, derived from their connection with fields:

Definition 5.12. A model of $CR \cup SIP \cup Ril$ is called a *meadow*.

All fields are clearly meadows but not conversely (as the initial meadow is not a field). In fact, the theorem proves a normal form theorem for meadows.

6. *Concluding Remarks*

6.1. OPEN PROBLEMS. The rational numbers are not well understood computationally or logically, even in the case of equational logic, possibly the simplest logic. We failed to obtain answers to the following problems:

PROBLEM 6.1. Does the totalized field Q_0 of rational numbers have a decidable equational theory?

In connection with algebraic specifications, the following is related to Problem 6.1. In fact, its positive solution would, by general specification theory, solve Problem 6.1.

PROBLEM 6.2. Does the totalized field Q_0 have a finite basis, that is, an ω-complete equational initial algebra specification?

The following problem is quite basic:

PROBLEM 6.3. Is there a finite equational specification of the totalised field Q_0, without hidden functions, which constitutes a complete term rewriting system?

We know from our Bergstra and Tucker [1995] that there exists such a specification with hidden functions.

Equations over Q_0 are called *diophantine equations*, just as equations over the integers are. We do not know the answer to this question:

PROBLEM 6.4. Does the totalized field Q_0 of rational numbers have a decidable diophantine theory, that is, can one decide whether or not $\exists x_1, \ldots, x_n[t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)]$?

If the diophantine theory of the totalized field of rationals is decidable (Problem 6.4), then the diophantine theory of the ring of rationals is also decidable (as it is the syntactic subtheory *without* division), and this latter question is a long standing open problem. Perhaps it is easier to show that Problem 6.4 is undecidable.

The specifications we have presented lead to questions, for instance:

PROBLEM 6.5. Does the specification $CR \cup SIP$ admit Knuth–Bendix completion?

Questions proliferate as one reflects on the number of algebras based on rational numbers.

PROBLEM 6.6. Is there a finite equational specification of the algebra $Q_0(i)$ of complex rational numbers, without hidden functions?

It is in fact possible to provide an initial algebra specification using the complex conjugate cc as an hidden function: see Bergstra and Tucker [2006a]. In the matter of term rewriting, we do not know the answer to this question:

PROBLEM 6.7. Is there a finite equational specification of the algebra $Q_0(i, cc)$, (without further hidden functions), which constitutes a complete term rewriting system?

Although there seems to be little work with this precise focus (e.g., Contejean et al. [1997]), a great deal is known about computable fields (see Stoltenberg-Hansen and Tucker [1999b]).

6.2. RELATED AND FUTURE WORK. It seems to us that an important task for the theory of algebraic specifications—and for formal methods in general—is this:

PROBLEM 6.8. To create a comprehensive theory of computing, specifying and reasoning with systems based on continuous data. Ideally, the theory should integrate discrete and continuous data.

At present, this is a huge and complicated task because computation, specification and verification on continuous data are all active research areas with disparate agendas. In fact, the task is a challenge in the special case of real numbers. The existing algebraic specification literature on the reals is limited. One of the earliest attempts at an axiomatic specification of any data type was the study of computer reals in van Wijngaarden [1966]. In Roggenbach et al. [2004], there is an axiomatization designed for the algebraic specification language CASL. In Tucker and Zucker [2002], there is a specification using infinite terms.

There is some progress on the question: Can all computable functions on continuous data be algebraically specified? In Tucker and Zucker [2005], it is shown that a computably approximable function on a complete metric algebra can be specified by a form of conditional equations. In fact it is shown there is one universal set of equations that can specify all computably approximable functions. (See Tucker and Zucker [2004] for the compact case and Tucker and Zucker [2005] for the general case.) There are many notions of computable function on the real numbers: see Tucker and Zucker [2000].

Obviously, technically, the specification theory of rational arithmetics is a basic subject for these tasks. If the rational numbers are the data type for measuring in units and subunits then the real numbers can be seen as the data type for *the process of measuring to arbitrary accuracy*, the measuring procedures being modeled by Cauchy sequences.

Our specification $CR \cup SIP$ draws attention to division by zero. Division by zero has been studied by Setzer [1997] in which he proposed the concept of *wheels*, a sophisticated modification of integral domains with constants for infinity and undefined, and division by zero with $0^{-1} = \infty$. Setzer's idea has been taken up in Carlström [2004].

For algebraic specification there is a great interest in limited types of first order formulae that are "close" to equations. Of course, conditional equations are an important example since they have initial models; another example of formulae are *multi-equations* studied by Adamek et al. [2002].

The problem is connected to many others such as the algebraic approaches to numerical software for scientific simulation, in Haveraaen [2000] and Haveraaen et al. [2005], and to 3D and 4D volume graphics, in Chen and Tucker [2000]. In fact, it is not an uncommon view that the problem of integrating discrete and continuous computation is a barrier to progress in computer science and its application.

REFERENCES

ADAMEK, J., HEBERT, M., AND ROSICKY, J. 2002. On abstract data types presented by multiequations. *Theoret. Comput. Sci. 275*, 427–462.

BERGSTRA, J. A. 2006. Elementary algebraic specifications of the rational function field. In *Logical approaches to computational barriers. Proceedings of Computability in Europe 2006*, A. Beckmann et al. Eds. Lecture Notes in Computer Science, vol. 3988, Springer-Verlag, New York, 40–54.

BERGSTRA, J. A., AND TUCKER, J. V. 1982. The completeness of the algebraic specification methods for data types. *Inf. Cont. 54*, 186–200.

BERGSTRA, J. A., AND TUCKER, J. V. 1983. Initial and final algebra semantics for data type specifications: Two characterisation theorems. *SIAM J. Comput. 12*, 366–387.

BERGSTRA, J. A., AND TUCKER, J. V. 1987. Algebraic specifications of computable and semicomputable data types. *Theoret. Comput. Sci. 50*, 137–181.

BERGSTRA, J. A., AND TUCKER, J. V. 1995. Equational specifications, complete term rewriting systems, and computable and semicomputable algebras. *J. ACM 42*, 1194–1230.

BERGSTRA, J. A., AND TUCKER, J. V. 2005. The rational numbers as an abstract data type. Res. Rep. PRG0504, Programming Research Group, University of Amsterdam, August 2005, or Tech. Rep. CSR12-2005, Department of Computer Science, University of Wales, Swansea, August 2005.

BERGSTRA, J. A., AND TUCKER, J. V. 2006a. Elementary algebraic specifications of the rational complex numbers. In *Goguen Festschrift*, K. Futatsugi et al., Eds. Lecture Notes in Computer Science, vol. 4060. Springer-Verlag, New York, pp. 459–475.

BERGSTRA, J. A., AND TUCKER, J. V. 2006b. Division safe calculation in totalised fields. Res. Rep. PRG 0605, Programming Research Group, University of Amsterdam, September 2006 or Tech. Rep. CSR 14-2006, Department of Computer Science, University of Wales Swansea, September 2006.

CALKIN, N., AND WILF, H. S. 2000. Recounting the rationals. *Amer. Math. Monthly 107*, 360–363.

CARLSTRÖM, J. 2004. Wheels - On division by zero. *Math. Struct. Comput. Sci. 14*, 143–184.

CHEN, M., AND TUCKER, J. V. 2000. Constructive volume geometry. *Computer Graphics Forum 19*, 281–293.

CONTEJEAN, E., MARCHE, C., AND RABEHASAINA, L. 1997. Rewrite systems for natural, integral, and rational arithmetic. In *Rewriting Techniques and Applications 1997*. Lecture Notes in Computer Science vol. 1232. Springer-Verlag, Berlin, Germany, pp. 98–112.

DICKSON, L. E. 1952. *History of the Theory of Numbers*. Chelsea, New York.

GOGUEN, J. A., THATCHER, J. W., AND WAGNER, E. G. 1978. An initial algebra approach to the specification, correctness and implementation of abstract data types. In *Current Trends in Programming Methodology. IV. Data Structuring* R.T. Yeh, Ed., Prentice-Hall, Engelwood Cliffs, pp. 80–149.

HARRISON, J. 1998. *Theorem Proving with the Real Numbers*, Springer-Verlag, New York.

HAVERAAEN, M. 2000. Case study on algebraic software methodologies for scientific computing. *Sci. Prog. 8*, 261–273.

HAVERAAEN, M., FRIIS, H. A., AND MUNTHE-KAAS, H. 2005. Computable scalar fields: A basis for PDE software. *J. Logic Alg. Prog. 65*, 36–49.

HODGES, W. 1993. *Model Theory*. Cambridge University Press, Cambridge, UK.

MEINKE, K., AND TUCKER, J. V. 1992. Universal algebra. In *Handbook of Logic in Computer Science. Volume I: Mathematical Structures,* S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 189–411.

MESEGUER, J., AND GOGUEN, J. A. 1985. Initiality, induction and computability. In *Algebraic Methods in Semantics*. M. Nivat and J. Reynolds, Eds. Cambridge University Press, Cambridge, pp. 459–541.

KLOP, J. W. 1992. Term rewriting systems. In *Handbook of Logic in Computer Science. Volume 2: Mathematical Structures*, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 1–116.

MOSS, L. 2001. Simple equational specifications of rational arithmetic. *Discr. Math. Theoret. Comput. Sci. 4*, 291–300.

ROGGENBACH, M., SCHRÖDER, L., AND MOSSAKOWSKI, T. 2004. Specifying real numbers in CASL. In *Recent Trends in Algebraic Development Techniques. 14th International Workshop (WADT '99)* (Chateau de Bonas, Sept. 15–18, 1999), D. Bert, C. Choppy, and P. D. Mosses, Eds. Lecture Notes in Computer Science, vol. 1827. Springer-Verlag, Berlin, 146–161.

SETZER, A. 1997. Wheels. Manuscript, 8 pp. Download at: http://www.cs.swan.ac.uk/csetzer.

STOLTENBERG-HANSEN, V., AND TUCKER, J. V. 1995. Effective algebras. In *Handbook of Logic in Computer Science. Volume IV: Semantic Modelling*, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 357–526.

STOLTENBERG-HANSEN, V., AND TUCKER, J. V. 1999. Computable rings and fields. In *Handbook of Computability Theory*, E. Griffor, Ed. Elsevier, North-Holland, Amsterdam, The Netherlands, pp. 363–447.

STOLTENBERG-HANSEN, V., AND TUCKER, J. V. 1999. Concrete models of computation for topological algebras. *Theoret. Comput. Sci. 219*, 347–378.

TERESE, 2003. *Term Rewriting Systems*. Cambridge Tracts in Theoretical Computer Science 55, Cambridge University Press, Cambridge, UK.

TUCKER, J. V., AND ZUCKER, J. I. 2000. Computable functions and semicomputable sets on many sorted algebras. In *Handbook of Logic for Computer Science. Volume V: Logic and Semantical Methods*, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 317–523.

TUCKER, J. V., AND ZUCKER, J. I. 2002. Infinitary initial algebraic specifications for stream algebras. In *Reflections on the Foundations of Mathematics: Essays in honour of Solomon Feferman*, W. Sieg, R. Somer and C. Talcott, Eds. Lecture Notes in Logic, Vol. 15, Association for Symbolic Logic, pp. 234–253.

TUCKER, J. V., AND ZUCKER, J. I. 2004. Abstract versus concrete computation on metric partial algebras. *ACM Trans. Computat. Logic 5*, 4, 611–668.

TUCKER, J. V., AND ZUCKER, J. I. 2005. Computable total functions on metric algebras, universal algebraic specifications and dynamical systems. *J. Alg. Logic Prog. 62*, 71–108.

WECHLER, W. 1992. *Universal algebra for computer scientists*. EATCS Monographs in Computer Science. Springer-Verlag, New York.

VAN WIJNGAARDEN, A. 1966. Numerical analysis as an independent science. *BIT 6*, 68–81.

WIRSING, M. 1990. Algebraic specifications. In *Handbook of Theoretical Computer Science. Volume B: Formal Models and Semantics*, J. van Leeuwen, Ed. North-Holland, Amsterdam, The Netherland, pp. 675–788.

RECEIVED SEPTEMBER 2005; REVISED JANUARY 2007; ACCEPTED JANUARY 2007